PRIMER EJERCICIO <u>PARTE TEÓRICA</u> DEL PROCESO SELECTIVO DE

B2 ANALISTA PROGRAMADOR SSII, SISTEMAS, REDES, SEG. RED, SEG. INFORMA, (ORDEN 2)

DE LA UNIVERSIDAD COMPLUTENSE DE MADRID

Concurso-Oposición Libre
Resolución de fecha 20-11-2024

09 de JUNIO de 2025

1. **¿Cuál NO es un modelo de calidad de servicio (QoS) en una arquitectura de redes?**
   - **a)** Best-effort
   - **b)** DiffServ (Differentiated Services)
   - **c)** IntServ (Integrated Services)
   - **d)** PriServ (Priority Services)

2. **¿Qué significa el 2 en la regla de la copia de seguridad 3-2-1?**
   - **a)** Deben hacerse 2 copias de datos
   - **b)** Deben utilizarse 2 formatos o soportes distintos
   - **c)** Las copias de seguridad deben almacenarse en 2 ubicaciones distintas
   - **d)** Deben utilizarse 2 herramientas diferentes para la realización de las copias de seguridad

3. **El protocolo LACP (Link Aggregation Control Protocol – IEEE 802.3ad):**
   - **a)** Permite el establecimiento de redes lógicas Ethernet en infraestructuras Ethernet nativas para mantener dinámicamente la topología entre nodos
   - **b)** Se desarrolló para minimizar la posición dominante de las tarjetas de red de Cisco y compatibilizarlas con las de sus entonces rivales: Alcatel-Lucent, Aruba, IBM, ...
   - **c)** Permite combinar varias conexiones de red físicas en una sola conexión lógica para aumentar el rendimiento y proporcionar redundancia
   - **d)** Proporciona conmutación modo activo/pasivo en las conexiones de red físicas para ofertar alta disponibilidad

4. **Con respecto a la virtualización, podemos afirmar que un hipervisor de tipo 1:**
   - **a)** Ocupa el lugar de un sistema operativo host y programa los recursos de las máquinas virtuales directamente en el hardware
   - **b)** También llamado “alojado”, permite múltiples lenguajes de programación sobre el sistema operativo host
   - **c)** Siempre es open source por compatibilidad con el sistema operativo host
   - **d)** Se ejecuta por encima del sistema operativo convencional como una capa de software o una aplicación

5. **¿Cuál de las siguientes afirmaciones sobre la estructura de una dirección IPv6 es correcta?**
   - **a)** Una dirección IPv6 tiene un tamaño fijo de 64 bits
   - **b)** Las direcciones IPv6 se representan en notación decimal
   - **c)** Las direcciones IPv6 no pueden contener ceros a la izquierda en sus grupos
   - **d)** Una dirección IPv6 se compone de ocho grupos de cuatro dígitos hexadecimales

6. **Según la guía CCN-STIC 836 Seguridad en Redes Privadas Virtuales (VPN), la VPN de acceso remoto:**
   - **a)** Se implementa con un servidor VPN en cada extremo de la comunicación
   - **b)** Precisa que los equipos cliente deben tener instalado y correctamente configurado el software VPN y deben autenticarse antes de poder usarla
   - **c)** Se emplea para establecer conexiones seguras entre dos equipos, protegiendo el tráfico desde un extremo al otro
   - **d)** Se emplea para proteger las comunicaciones entre dos redes, a través de una red pública, manteniendo la seguridad y enrutando las comunicaciones

---

7. **¿Cuál de las siguientes NO puede ser considerada una herramienta de gestión de la configuración?**
   - **a)** Ansible
   - **b)** Puppet
   - **c)** Chef
   - **d)** Flume

8. **El rango completo asignado por IANA a direcciones IPv4 multicast es:**
   - **a)** 224.0.0.0/4
   - **b)** 232.0.0.0/8
   - **c)** 239.0.0.0/8
   - **d)** 240.0.0.0/4

9. **¿Cuál es la característica principal de la criptografía asimétrica?**
   - **a)** Utiliza una sola clave compartida entre emisor y receptor
   - **b)** Emplea dos claves diferentes: una privada y una pública
   - **c)** Solo cifra datos, no permite firmar digitalmente
   - **d)** Es más rápida que la criptografía simétrica

10. **¿Qué garantías ofrece una firma digital válida en un sistema de criptografía asimétrica?**
    - **a)** Autenticidad, integridad y no repudio
    - **b)** Compresión, velocidad de transmisión y anonimato
    - **c)** Confidencialidad, ocultamiento y cifrado simétrico
    - **d)** Privacidad, almacenamiento seguro y sincronización de datos

11. **¿Qué es una clave concertada en el contexto de la administración electrónica?**
    - **a)** Un sistema de doble clave que cifra la información entre dos administraciones públicas
    - **b)** Una contraseña generada aleatoriamente por el sistema para acceder a cualquier servicio público
    - **c)** Datos proporcionados por la Administración que obran en poder del interesado y que solo él debería conocer
    - **d)** Un identificador público utilizado para firmar digitalmente documentos oficiales

12. **¿Qué es una PKI (Infraestructura de Clave Pública)?**
    - **a)** El conjunto de elementos de software, hardware, procedimientos, políticas y personal cuyo objetivo es crear, almacenar, distribuir y revocar certificados digitales de clave pública
    - **b)** Un protocolo de red exclusivo para cifrar las comunicaciones entre routers
    - **c)** Un sistema operativo dedicado exclusivamente a la gestión de redes privadas
    - **d)** Una base de datos que almacena contraseñas de todos los usuarios de un sistema informático

13. **¿Cuántos bits se usan en una trama ethernet para identificar una VLAN?**
    - **a)** 4
    - **b)** 8
    - **c)** 12
    - **d)** 16

14. **Si dispone de la siguiente especificación de red IPv4: 147.96.96.0/22 ¿señale cuál de las siguientes IPs podría ser la de un enrutador de dicha red?**
    - **a)** 147.96.96.7
    - **b)** 147.96.94.7
    - **c)** 147.96.96.265
    - **d)** 147.96.100.1

15. ¿Cuántas capas tiene el modelo OSI?

a) 4

b) 6

c) 7

d) 8

16. ¿Cuál de los siguientes es un ejemplo de ataque de fuerza bruta?

a) Explotar una vulnerabilidad conocida en un software

b) Probar múltiples combinaciones de contraseñas hasta encontrar la correcta

c) Redirigir el tráfico de un sitio web a otro malicioso

d) Manipular una base de datos para obtener acceso no autorizado

17. El Esquema Nacional de Interoperabilidad, según el artículo 156 de la Ley 40/2015, de 1 de octubre, comprende:

a) Las obligaciones a que están sujetas las Administraciones Públicas para garantizar una correcta interoperabilidad de sus sistemas, redes y aplicaciones en su relación con la ciudadanía

b) Los criterios técnicos que han de seguir las Administraciones Públicas en el desarrollo, contratación ypuesta a disposición de herramientas tecnológicas por los departamentos ministeriales

c) El conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad

d) La política de seguridad en la utilización de medios electrónicos por las Administraciones Públicas

18. En el ámbito de las políticas de backup (respaldo), señale la respuesta correcta:

a) La copia de seguridad incremental realiza copia de los archivos y directorios que han sido modificados desde la última copia completa

b) La copia de seguridad incremental es igual que la copia de seguridad diferencial, pero sin borrar el bit de modificado

c) La copia de seguridad incremental ahorra tiempo pero ocupa el mismo espacio en cinta con respecto a la copia de seguridad completa

d) La copia de seguridad incremental realiza copia de los archivos y directorios que han sido modificados desde la última copia, ya sea completa o no

19. ¿Qué tipo de cifrado utiliza HTTPS para asegurar la comunicación entre el cliente y el servidor?

a) Cifrado asimétrico en la negociación, seguido de cifrado simétrico en la transmisión de datos

b) Cifrado simétrico únicamente, usando una clave precompartida

c) Cifrado por flujo, utilizando una clave de sesión única para cada mensaje

d) Cifrado de capa de transporte sin autenticación del servidor

20. ¿Cuál es la guía que articula el mecanismo de Declaración y Certificación de Conformidad con el Esquema Nacional de Seguridad (ENS),

a) Guía CCN-STIC 812

b) Guía CCN-STIC 823

c) Guía CCN-STIC 809

d) Guía CCN-STIC 803

PREGUNTAS DE RESERVA

21. ¿Qué herramienta se utiliza para detectar y prevenir intrusiones en una red?

a) Cortafuegos (Firewall)

b) Sistema de detección de intrusiones (IDS)

c) Protocolo de seguridad IP (IPsec)

d) Red privada virtual (VPN)

22. ¿Qué versión de LDAP se recomienda utilizar actualmente por ser la más estable y ampliamente soportada?

a) LDAPv3

b) LDAPv1

c) LDAP 5.2

d) LDAP 2008

23. ¿Cómo se denomina al ataque consistente en el envío masivo de tramas a un switch con dirección MAC aleatoria?

a) ARP poisoning

b) MAC spoofing

c) ARP watch

d) MAC flooding

24. En relación al ámbito de la seguridad de la red de una organización, podríamos afirmar que:

a) IDS (Intrusion Detection System) es un servidor en la red que bloquea los accesos no autorizados

b) IPS (Intrusion Prevention System) es un software que se utiliza para un análisis forense de los ataques y accesos no autorizados

c) SIEM (Security Information and Event Management) es un software que engloba la gestión de información de seguridad y la gestión de eventos

d) IGS (Intrusion Gateway System) combina las tareas de un IDS y un IPS, proporcionando un análisis en tiempo real de las alertas de seguridad generadas por los distintos dispositivos hardware y software de la red

25. En las comunicaciones Wi-Fi ¿En qué estándar se introdujo la tecnología de red Wi-Fi mallada (mesh)?

a) 802.11i

b) 802.11ad

c) 802.11e

d) 802.11s